WWW.SCIAM-MAGAZINE.NAROD.RU

Занимательный компьютер

О шифровальных и дешифровальных машинах. Часть I

А.К. ДЬЮДНИ

«Что бы ни придумал один человек, другой сможет это раскрыть», — говорил Шерлок Холмс, герой произведений Артура Конан-Дойла.

СЛЕДУЕТ ЛИ рассматривать эти слова знаменитого детектива как хладнокровное выражение уверенности в своей способности расшифровывать секретные коды или это скорее констатация исторического факта? Несомненно, что начиная со времен, когда была изобретена письменность, вплоть до середины нашего столетия, коды, придуманные одними людьми, чтобы скрыть смысл важных военных или служебных сообщений, в конце концов разгадывались другими. Перед началом второй мировой войны кодировать сообщения стали с помощью машин, но и с их приходом ситуация по сути не изменилась. Перефразируя Холмса, можно сказать: «То, что закодирует одна машина, другая раскодирует».

Данная статья — первая из двух статей, посвященных секретным шифрам, — как раз завершается рассуждением о единоборстве кодирующих и декодирующих машин. На одной стороне такого поединка выступает машина «Enigma» (загадка), которая применялась 50 лет назад в вооруженных силах держав «оси Берлин — Рим», на другой — машина «Bombe» (бомба). Как увидим, неустанно тикающая «Bombe» медленно, но верно шла к победе, правда, не без помощи людей, — в том числе Алана М. Тьюринга, одного из основателей информатики и вычислительной техники. В следующем номере журнала я продолжу эту тему и расскажу о том, как компьютеры применяются в наше время для шифровки и дешифровки секретных сообщений.

Исторически вначале применялись шифры, преобразующие сообщение на обычном естественном языке в закодированную форму, или шифрованный текст, путем замены одних букв алфавита другими. Например, в так называемом шифре Цезаря это делалось в соответствии с простой схемой нумерации. Если пронумеровать буквы латинского алфавита ($A, B, C, \ldots$) от 0 до 25, то, задав какое-нибудь определенное число, скажем 13, можно прибавлять его к числам, соответствующим каждой букве исходного текста на естественном языке. Получаемые суммы будут представлять букву шифрованного текста. Если какая-нибудь сумма окажется больше 25, то, вычтя из нее 26, получим число, принадлежащее диапазону от 0 до 25. Так, например, X (буква номер 23) будет кодироваться как K (буква номер 10), потому что $23 + 13 = 36$ и $36 - 26 = 10$.

Говорят, что Юлий Цезарь пользовался этим шифром, чтобы сообщения с арены боевых действий не могли стать достоянием противника, если бы они попали в его руки. Приведем одно из таких возможных сообщений римского полководца с просьбой прислать подкрепление на естественном языке и в зашифрованном виде:

SEND MMCC REINFORCEMENTS
FRAQ ZZPP ERVASBEPRZRAGF

Для того чтобы можно было пользоваться такой системой, предполагаемый получатель шифровки должен иметь к ней ключ. В данном случае ключ — это буква N, или буква под номером 13. Зная эту букву, получатель сможет восстановить исходный текст, просто вычитая 13 из чисел, соответствующих каждой букве шифрованного текста.

Сообщение может попасть в руки противника (будем называть его дешифровщиком), который попытается расшифровать его, подставляя по очереди все буквы алфавита в качестве ключа. Если противник попытается расшифровать сообщение, предположив, что ключом является буква B, то результат будет следующим:

TFOE NNDD SFJOGPSDFNFOUT

Поскольку получилась бессмыслица, дешифровщик попытается применить другой ключ, и в конце концов он наткнется на букву N, которая превратит бессмыслицу в разумную фразу на английском языке.

На первый взгляд может показаться, что компьютер не способен помочь в расшифровке сообщений, закодированных шифром Цезаря, поскольку машина при переборе всевозможных ключей и подстановке их в

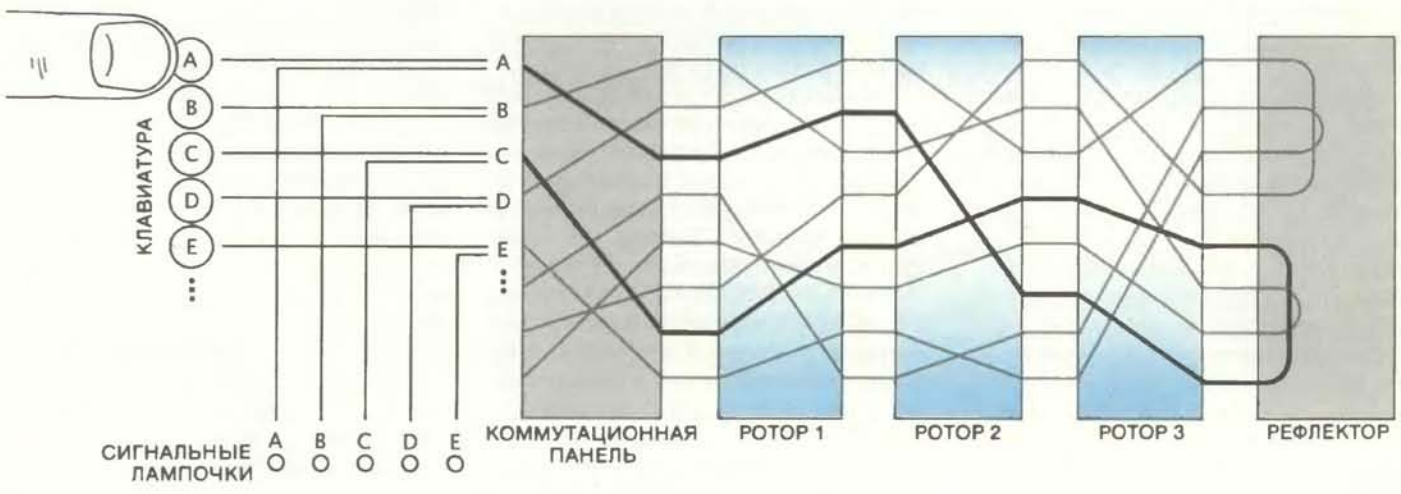


Схема машины «Enigma»

WWW.SCIAM-MAGAZINE.NAROD.RU

зашифрованный текст не сможет отличить бессмыслицу от текста, имеющего определенное значение. Однако компьютер можно снабдить «словарем», который по крайней мере позволит ему установить, содержит ли закодированное сообщение слова естественного языка. Но существует и другой, более мощный инструмент расшифровки: статистика.

Каждая буква алфавита встречается обычно в текстах данного языка с определенной частотой (измеряемой частотностью). Например, частотность первых трех букв латинского алфавита в текстах на английском языке составляет в среднем соответственно 8, 1,5 и 3%. Чаще всего встречается буква *E*, ее частотность равна 13%. (Полная таблица частотности всех букв в англоязычных текстах приведена на рисунке справа.)

В шифровке гипотетического сообщения Цезаря чаще всего встречается буква *R*, а именно 4 раза. Расшифровывающая программа может поэтому предположить, что *R* подставлено вместо *E*. Поскольку разность между числовыми представлениями букв *R* и *E* равна 13, программа может далее предположить, что ключом шифра является буква *N*.

В данном случае такая программа окажется правой, однако во многом это результат везения. В реальной практике статистическими закономерностями при расшифровке можно успешно пользоваться только тогда, когда в распоряжении имеются достаточно длинные шифрованные тексты. Помимо определения наиболее вероятного кандидата на букву *E* программа могла бы также попытаться найти буквы, заменяющие *T*, *A* и *Q*, которые тоже часто встречаются в английском языке. Она могла бы даже сопоставить распределение встречаемости букв в шифрованном тексте со статистическим распределением тех же букв в обычном тексте, чтобы выявить наиболее вероятные ключи.

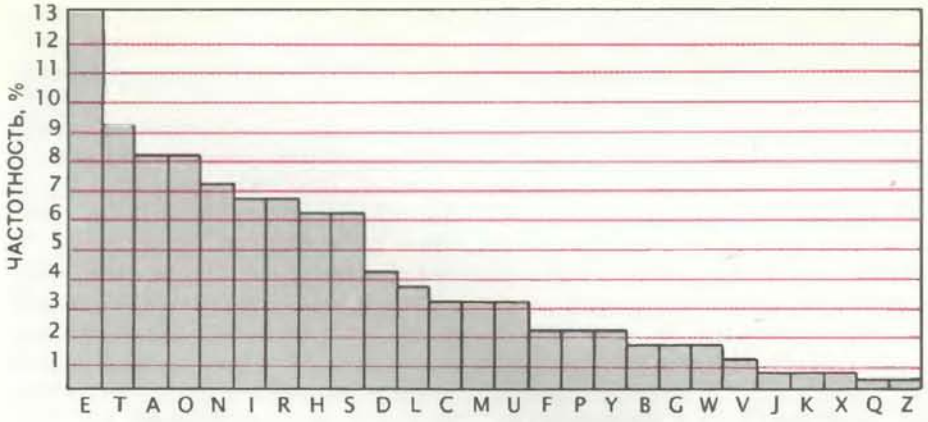
Блез де Вижинер, французский криптограф XVI в., усложнил код Цезаря, предложив менять ключ с определенной периодичностью. Кодируя сообщение по методу Вижинера, букву-ключ изменяют для каждой буквы исходного текста в последовательности, соответствующей списку букв-ключей. По существу ключом шифра является эта последовательность букв.

Предположим, например, что ключом является последовательность CLEF, которой соответствует числовая последовательность 2, 11, 4, 5. Чтобы зашифровать сообщение при помощи этой последовательности, нужно разбить буквы исходного текста на группы из четырех букв каждая. Затем нужно прибавить 2 к числовому представлению первой буквы в каждой группе, 11 — второй, 4 — третьей и 5 — четвертой. Так же как и в шифре Цезаря, получающиеся суммы представляют числовые значения букв зашифрованного текста. Приведем пример, иллюстрирующий, каким образом шифр Вижинера преобразует исходный текст в шифровку:

ключ: CLEFCLEFCLEFCLEF
исходный текст: SENDINTHECAVALRY
шифрованный текст:
UPRIKYXMGNEACWVD

Шифрованные сообщения могут представлять собой либо непрерывную цепочку символов, как в предыдущем примере, либо их можно разбить на отдельные блоки. В любом случае предполагается, что получатель сумеет сгруппировать расшифрованные символы в слова.

Если расшифровывающему известен период ключа (число букв в ключевой последовательности) шифра Вижинера, он может декодировать сообщение, применив по существу тот же метод, которым пользуются для декодирования шифра Цезаря. Но в данном случае процесс займет значительно больше времени. Чтобы декодировать приведенный выше текст, зашифрованный по методу Вижинера, расшифровывающая компьютерная программа должна будет построить четыре распределения по буквам: одно для каждой четвертой буквы в последовательности, начинающейся с *U*, одно для каждой четвертой буквы в последовательности, начинающейся с *P*, и т.д. Затем программа сравнит каждое из полученных распределений со стандартным статистическим распределением встречаемости букв, чтобы определить каждую из четырех букв ключевой последовательности. Фактически задача сводится к расшифровке четырех отдельных шифров Цезаря. Если расшифровывающему не известен период ключевой последовательности, декодирование займет еще больше времени, поскольку необходимо будет перебрать все возможные периоды. В данном случае возможность воспользоваться компьютером дает существенное преимущество, потому что компьютер очень хорошо справляется с многократно повторяющимися процедурами.



Частотность букв латинского алфавита в обычном английском тексте

Само собой разумеется, что если мы имеем дело с короткими сообщениями или длинными ключевыми последовательностями букв, то необходимо будет набрать большое число сообщений, прежде чем расшифровка шифра Вижинера увенчается успехом. И наоборот, если применяются короткие ключевые последовательности, компьютер почти наверняка восстановит исходный текст, даже если ему предъявить не очень длинные сообщения.

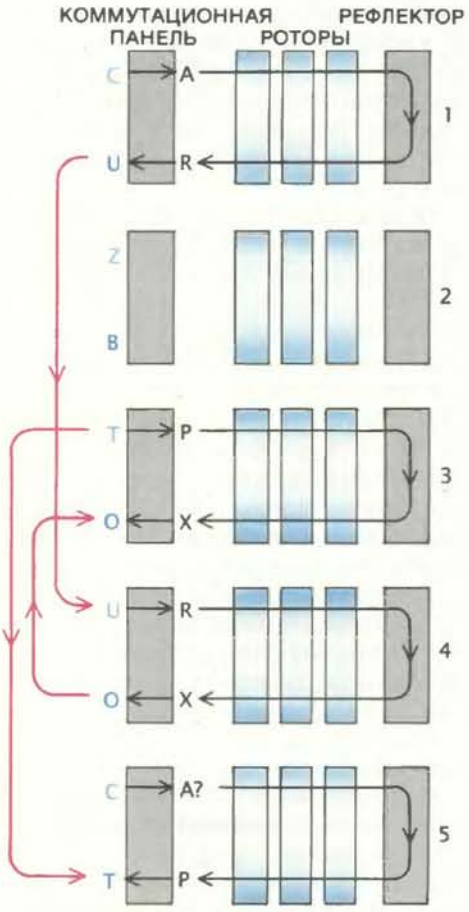
Теперь, минуя множество замысловатых систем кодирования, изобретенных в период между XVI и серединой XX в., перейдем к рассмотрению немецкой машины «Enigma», с которой связана наиболее серьезная и крупномасштабная попытка расшифровки, когда-либо предпринимавшаяся до тех пор. Машина применялась фашистской Германией во время второй мировой войны для шифровки передаваемых по радио сообщений (эти сообщения сами передавались в телеграфном коде), которыми обменивались полевые и штабные подразделения. Поскольку радиосообщения легко перехватить, располагая радиоприемником, настроенным на соответствующую частоту, необходимость шифровки сообщений очевидна.

Основная машина системы «Enigma» состояла из алфавитной клавиатуры, трех «роторов», «рефлектора» и набора из 26 лампочек-индикаторов, по одной на каждую букву алфавита (см. рисунок на с. 112). Ротор представлял собой зубчатое колесо, через которое проходили провода, соединяющие 26

WWW.SCIAM-MAGAZINE.NARODRU

контактов на одной стороне ротора с таким же количеством контактов на другой его стороне. Соединения были выбраны произвольно, но затем они уже не менялись. В каждом из возможных положений ротор представлял какую-то конкретную систему перестановок для 26 возможных электрических сигналов от клавиатуры (по одному для каждой буквы). Например, ротор мог послать сигнал, представляющий букву A на контакт, соответствующий букве R, сигнал, представляющий B, на контакт, соответствующий D, и т.д. Второй ротор, с другим расположением проводников и находящийся, вообще говоря, в другом положении, принимая сигнал от первого ротора, подвергал его еще одной перестановке. Последний, третий ротор аналогичным образом осуществлял еще одну перестановку.

Пройдя через три ротора, сигнал поступал на рефлектор: систему проводников, соединяющую каждый контакт с другим контактом на задней стороне третьего ротора. Таким образом, рефлектор посылал сигнал обратно, по другому пути, через три ротора. Проходя от ротора к ротору в обратном порядке, сигнал претерпевал еще три изменения. Когда сигнал, наконец, выходил из системы роторов, он поступал на лампочку-индикатор.



«Bombe» пытается определить схему соединений на коммутационной панели шифровальной машины

Ключевым свойством машины «Enigma» был обратимый характер ее действия: если она кодировала букву R как Q, то, находясь в том же состоянии, она кодировала букву Q как R. Такая обратимость означала, что шифрованный текст, отпечатанный на клавиатуре машины, преобразовывался в исходный текст, при условии, что при декодировании машина находилась в том же состоянии, что и во время кодирования. Как следствие, шифровка и дешифровка сообщений сводились к одной и той же простой операции — установке роторов в правильное положение. Свойство обратимости, обеспечившее максимальное удобство для операторов машины, оказалось, как мы увидим в дальнейшем, роковым для этой системы кодирования.

Шифровки, посылаемые с помощью «Enigma», было особенно трудно декодировать еще и потому, что первый ее ротор автоматически поворачивался на одну позицию после каждой отпечатанной буквы. После того как клавиши были нажаты 26 раз, ротор возвращался в исходное положение, но зато второй ротор перемещался при этом в новое положение. Аналогичным образом, когда второй ротор поворачивался 26 раз, третий ротор также поворачивался на одну позицию. Система роторов по существу работала подобно одометру (курвиметру) в автомобиле. Благодаря такому механизму каждая буква исходного сообщения кодировалась по новой системе подстановки. Всего машина перебирала $26 \times 26 \times 26 = 17\,576$ различных подстановок, прежде чем вернуться к исходному состоянию.

Такое кодирование напоминает метод Вижинера, однако в данном случае шифр оказывается неизмеримо сложнее. Каждая буква ключевой последовательности шифра Вижинера также осуществляет перестановку алфавита, заменяя букву исходного текста другой буквой, числовое значение которой является суммой чисел, соответствующих букве исходного текста и ключевой букве. Однако в шифре Вижинера применяется столько перестановок, сколько букв насчитывает ключевая последовательность, после чего происходит возврат к первоначальному «состоянию». Другими словами, машина «Enigma» имела ключевую последовательность длиной 17 576 букв.

Если бы английским специалистам по расшифровке ничего не было известно о системе кодирования машины «Enigma», то разгадать ее шифр было бы практически невозможно. Статистический подход, основанный на средних значениях частотности букв в немецком языке, оказался бы бесполезным, поскольку любая буква исходного текста кодировалась поочередно любой буквой алфавита практически с одной и той же вероятностью. Однако англичане отнюдь не были в полном неведении относительно принципа, на котором была основана секретная кодирующая машина.

Еще перед войной французской разведке удалось добыть копии служебных инструкций для работающих с машиной. Французы передали эти материалы полякам, которые успешно воспользовались ими. Анализируя перехваченные немецкие радиосообщения с учетом имеющихся инструкций, польские специалисты сумели определить структуру соединений в трех роторах и рефлекторе машины. Благодаря этому было уже нетрудно определить сложную перестановку, являющуюся результатом совместного действия трех роторов, рефлектора и вторичного прохода через роторы, и тогда появилась возможность расшифровывать немецкие секретные сообщения — при условии, что было известно исходное состояние роторов. На самом деле исходные состояния машин польские специалисты могли определять по ежедневным шифрованным сообщениям, задававшим положение ротора на следующий день.

Хотя англичане и получили от поляков всю эту информацию, во время войны она оказалась уже недостаточной, так как перед самой войной немцы модифицировали свои машины системы «Enigma». Во-первых, они увеличили количество роторов до пяти. Поэтому, прежде чем пытаться декодировать перехваченные радиосообщения, нужно было определить, какие три из пяти взаимозаменяемых роторов были в машине. Во-вторых, в некоторых моделях машины, применявшихся в армии, была дополнительная «коммутационная панель», выполнявшая еще одну перестановку на шести или семи парах букв, перед тем как соответствующие электрические сигналы от клавиатуры достигали системы роторов и после того, как они ее покидали. Поляки, достигшие предела своих технических возможностей, после введения этих изменений вынуждены были отказаться от попыток расшифровывать секретные тексты.

Эту работу продолжили англичане, приняв эстафету от поляков. Вначале они собрали смешанную группу специалистов по шифрам и математиков

WWW.SCIAM-MAGAZINE.NAROD.RU

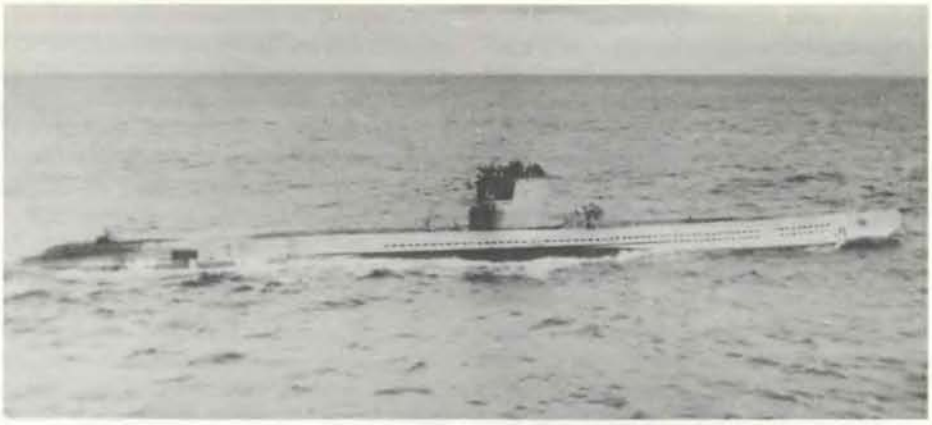
(в число которых входил также Тьюринг) в викторианской усадьбе в Бакингемшире, называемой Блетчли-Парк. Располагая сведениями о структуре соединений в роторах и рефлекторе машины, группа должна была раскрыть структуру коммутационной панели. Было решено применить так называемый метод вероятного слова.

Этот метод основывался на том факте, что в некоторых контекстах определенная последовательность символов перехваченного сообщения почти наверняка представляет известное слово. Шифровка, переданная из штаба немецкого военно-морского флота, могла содержать, например, блок из пяти букв, который логично интерпретировать (с достаточно большой вероятностью, что эта интерпретация будет правильной) как закодированное слово *U-boot* (сокращение от немецкого слова *Unterseeboot*, или подводная лодка).

Правильно догадавшись, что́ означает несколько слов шифрованного текста, можно было определить структуру контактов коммутационной панели, просто перепробовав все возможные соединения и выбрав из них то, которое давало бы нужное соответствие между зашифрованной и расшифрованной формой слов с уже известным значением. Но поскольку число возможных вариантов соединений на коммутационной панели для семи подстановок между парами букв все же больше миллиарда, Тьюринг понимал, что только быстродействующая машина сможет выполнить необходимый перебор.

Действительно, то, что Тьюринг решил воспользоваться машиной для расшифровки кода, сгенерированного другой машиной, уже не казалось чем-то удивительным. Поляки сами пользовались электромеханическими имитаторами машины «Enigma». Мерно пощелкивая, имитаторы переключались от одной «позиции» к другой, пытаясь определить, какая комбинация роторов воспроизводит данную перестановку. Звуки, производимые работающими имитаторами, напоминали тиканье часового механизма, поэтому их прозвали «бомбами».

Чтобы раскрыть структуру соединений коммутационной панели, была построена «бомба» нового типа. Машина «Bombe» представляла собой систему переключателей, или реле, которые перебирали все возможные варианты соединений на коммутационной панели в поисках логического соответствия имеющимся данным. В принципе проверка была простой. Рассмотрим, к примеру, пять машин системы «Enigma» и пронумеруем их от 1 до 5 (см. рисунок на с. 114). Роторы в этих пяти машинах расположены так, чтобы моделировать суммарное действие одной машины, которое она будет выполнять при наборе каждой буквы пятибуквенного слова. (Напомним, что исходное положение роторов машины, зашифровавшей слово, нам известно по данным, которые удалось получить разведке). Аналитики определили, что пятибуквенное слово шифровки CZTUC, вероятно, означает в исходном тексте слово UBOOT (подводная лодка). На основании этой информации предстояло найти те соединения на коммутационной панели, которые использовались в этот день для кодирования всех сообщений.



Немецкие подводные лодки времен второй мировой войны были оснащены машинами системы «Enigma»

Бомба Тьюринга начала бы с какого-нибудь произвольного предположения, скажем, что буква C на входной стороне коммутационной панели соединялась с буквой A на первом роторе. Допустим, далее, что «Enigma-1» преобразует букву A в R. Если наша гипотеза относительно значения слова правильна, то коммутационная панель должна заменять букву R на U и благодаря обратимости действия машины букву U на R.

Последний вывод означает, что коммутационная панель машины «Enigma-4» должна также заменять букву U в шифрованном тексте на R. Если машина 4 (ротор которой должен быть сдвинут на три позиции по отношению к машине 1) преобразует букву R, поступающую с коммутационной панели в X, то «Bombe» сразу же сделает вывод, что существует связь между буквами X и O, поскольку, по предположению, четвертая буква исходного текста — это O.

Этим выводом можно теперь воспользоваться при анализе действия машины в ее 3-м варианте, в котором она кодирует третью букву слова UBOOT. Если окажется, что машина 3 выдает букву X, когда получает на входе P, то мы устанавливаем, что на коммутационной панели существует связь между P и T, поскольку T является третьей буквой зашифрованного слова CZTUC.

Так как слово UBOOT заканчивается буквой T, «Bombe» приходит к критическому выводу: не завершает ли машина 5 логический цикл, преобразуя P в A, так чтобы коммутационная панель давала букву C, стоящую на последней позиции шифрованного слова? Если нет (как оно обычно и было), то гипотеза о том, что коммутационная панель связывала буквы C и A, оказывалась несостоятельной. В этом случае «Bombe» приняла бы следующую гипотезу, скажем, что C связана с B. Если и эта гипотеза оказалась бы несостоятельной, машина рассмотрела бы вариант, когда C связана с C и т.д. Действуя в таком ключе, бомба Тьюринга в конце концов должна раскрыть правильные соединения на коммутационной панели.

Шифрованное слово, рассмотренное в примере, относительно короткое и в наших машинах системы «Enigma» перестановки букв были выбраны таким образом, что их было удобно анализировать путем проверок на логическое соответствие. В действительности приходилось расшифровывать значительно более длинные сообщения, дававшие больше информации для логических заключений. Таким образом бомба Тьюринга могла в результате процесса дедукции раскрыть все связи на коммутационной панели. В этот момент она, наверное, прекращала тикать, сигнализируя о том, что сейчас произойдет взрыв — но, конечно, не в Блетчли-Парке.

Решение задачи о соединениях в коммутационной панели было лишь частью усилий по дешифровке, предпринятых Тьюрингом и его коллегами. Например, каждый день нужно было определять еще исходную установку роторов, а также некоторые другие параметры, от которых зависела работа машины «Enigma» и которые из-за недостатка места мы не

WWW.SCIAM-MAGAZINE.NARODU.RU

будем здесь обсуждать. Достаточно будет сказать, что группа специалистов, собранных в Блетчли-Парке, все время напряженно работала, расшифровывая различные версии шифров, применявшиеся немцами. Наверное, важнее все-таки было бы, что их работа, в которой они воспользовались машинами для расшифровки кодов, порожденных другой машиной, возвестила о начале новой эры, когда логические операции стали выполнять, машины, что в конечном итоге привело к современным компьютерам.

В следующей статье я продолжу эту криптологическую тему, рассказав о положении дел в этой области на сегодняшний день. А сейчас мне остается лишь добавить, что есть много энтузиастов, увлеченно занимающихся на досуге компьютерной криптологией. Некоторые из них даже написали программы, имитирующие машину «Enigma» и работу англичан по расшифровке ее кодов. Я хочу, в частности, поблагодарить Б. Милевски из Калифорнийского университета в Дейвисе, описавшего свой внушительный пакет программ CRYPTO, предназначенный для расшифровки кодов. В этом пакете есть, в частности, программа, расшифровывающая коды машины «Enigma» с одним ротором. Читатели могут попытаться составить собственные программы типа CRYPTO. Для них это будет хорошим практикумом в деле совершенствования своего мастерства в программировании.

В АВГУСТОВСКОМ номере журнала была помещена статья о решетчатых орнаментах, замысловатых узорах, которые плетутся на плоскости согласно строгим геометрическим правилам. Б.Уоллис из Портола-Вэлли (шт. Калифорния) придумал, как можно генерировать приблизительно такие же узоры на экране компьютера, накладывая друг на друга четыре квадратные решетки, сдвигаемые или вращаемые одна относительно другой. Программа, основанная на применении пифагоровых чисел (чисел, соответствующих сторонам прямоугольного треугольника), производит некий фантастический художественный эффект, подобный галлюцинации. Эффекты такого рода можно было бы получить из нескольких экранов с отверстиями, наложенных один на другой, вращаемых и сдвигаемых относительно друг друга.

Дж. Хоскинс, специалист по информатике из Университета Манитоба в Виннипеге (Канада), написала для своего микрокомпьютера программу, создающую решетчатые диаграммы ткани для каждого пересечения ее основы и утка. Программа позволяет ткачу сразу видеть, какой эффект то или иное перемежение нитей окажет на узор готовой ткани. Программа создает также диаграммы непосредственно по цифровым представлениям изображений.

Наконец, для увлекающихся игрой «Бой в памяти», сообщим, что III международный турнир по этой игре состоится 3—4 декабря в штаб-квартире Международного общества по игре «Бой в памяти» в Хантингтон-Биче (шт. Калифорния).

Наука и общество

Шунт не всегда выгоден

НЕКОТОРОЕ время считалось, что операция коронарного шунтирования может облегчить боли при стенокардии и улучшить качество жизни больного, повысив его способность переносить физические нагрузки. Однако продлевает ли она жизнь, оставалось под вопросом. Результаты проведенного недавно в европейских странах широкомасштабного обследования свидетельствуют, что такой эффект есть, однако со временем разница сглаживается. Поэтому операция рекомендуется главным образом в крайне тяжелых случаях.

Операция коронарного шунтирования состоит в том, что фрагмент какого-нибудь сосуда подсоединяется к пораженной венечной артерии в обход закупоренного участка, обеспечивая свободное течение крови к сердцу. Вопрос о преимуществах этого хирургического вмешательства стоит как перед обществом в целом, так и перед каждым конкретным врачом и пациентом. Действительно, за последний год в США только в больницах, не входящих в федеральную систему здравоохранения, сделано более 200 тыс. таких операций.

Недавно в журнале «New England Journal of Medicine» опубликованы последние результаты обширного обследования, которое ведется с 1973 г. в ряде медицинских центров европейских стран. В первые 3 года было набрано 767 больных стенокардией, и часть их (случайную выборку) лечили только терапевтическими методами, а другим делали операцию коронарного шунтирования, после чего обе группы пациентов наблюдались на протяжении 12 лет. Спустя 5 лет между ними была отмечена четкая, статистически значимая разница: среди оперированных больных умерли 8%, в то время как в контрольной группе — 17%. Однако через 12 лет различие оказалось меньшим: в первой группе остались в живых 71%, во второй 67%, причем статистическая значимость была гораздо меньшей.

При более подробном обследовании обеих групп выяснилось, что операция более всего продлевает жизнь пациентам с тяжелой ишемией сердца. К тяжелым относятся случаи сужения сразу нескольких венечных артерий, включая левую переднюю нисходящую — одну из главных ветвей коронарного кровообращения. Как считают авторы статьи, эти симптомы являются показаниями к раннему хирургическому вмешательству.

Чем подтверждается их вывод? В редакционном комментарии к статье Т.Киллип из Медицинского центра Бет Израэль в Бостоне (автор широко используемой классификации инфаркта миокарда) пишет: «Важный новый факт заключается в том, что операция коронарного шунтирования не всегда приносит больному продолжительное облегчение». По его мнению, это объясняется тем, что после операции трансплантат вырождается и продолжаются атеросклеротические изменения венечных артерий. Для устранения таких явлений обычно прибегают ко второму шунтированию, которое гораздо рискованнее первого.

Итак, можно сделать вывод, что больным с сильной коронарной недостаточностью операцию шунтирования нужно делать как можно быстрее, но в менее серьезных случаях следует как можно дольше воздерживаться от нее. «Задача врача — определить оптимальное время для хирургического вмешательства, если без него не обойтись», — считает Киллип.

Дрожжи и эстроген

ЧЕМ ОТЛИЧАЕТСЯ человек от дрожжей? На макроскопическом уровне разница между этими двумя организмами очевидна и весьма значительна, однако на уровне отдельной клетки начинает размываться. Если же сравнивать на молекулярном уровне гены, то преобладает скорее сходство, причем не только в структуре молекул, но и в процессах, регулирующих их функционирование. По крайней мере такое впечатление складывается в результате многочисленных исследований, в которых производился обмен регуляторными элементами ге-